California
TECHNOLOGY AGENCY
Office of Information Security

Information Security Officer Meeting

January 12, 2012

Meeting Agenda

----- Topics -----	
Opening Remarks	5 minutes
Statewide Security Program Updates	40 minutes
California Highway Patrol, Computer Crimes Investigations Unit Sgt. Kelly Dixon	20 minutes
Open Discussion	40 minutes
Q&A and Closing	15 minutes

Opening Remarks

- Happy New Year!
- Status of AIO/AISO Meetings
- Security Program and Policy Improvement Sub-Committee

Keith Tresh, Director and CISO

Organizational Update

- More organizational change on the horizon
- Governor's budget proposes to restructure Technology, General Services, and Human Resources into a new Government Operations Agency.
- Proposed changes are available at: http://www.ebudget.ca.gov/

Organizational Update *(Continued)*

- Technology Agency supports the proposal.

"By placing the Technology Agency together with the Department of General Services and the Department of Human Resources, the opportunity to collaborate on issues such as IT procurement and maintaining a capable IT work force becomes easier."

– Carlos Ramos, Secretary

Legislative Update

- SB 24 (Simitian)
  - Approved by Governor August 31, 2011
  - Effective January 2012
  - Requires more specific language in breach notifications
  - Requires an electronic copy of breach notification be provided to AG for a single incident involving 500+ individuals
- Chaptered legislation available at:

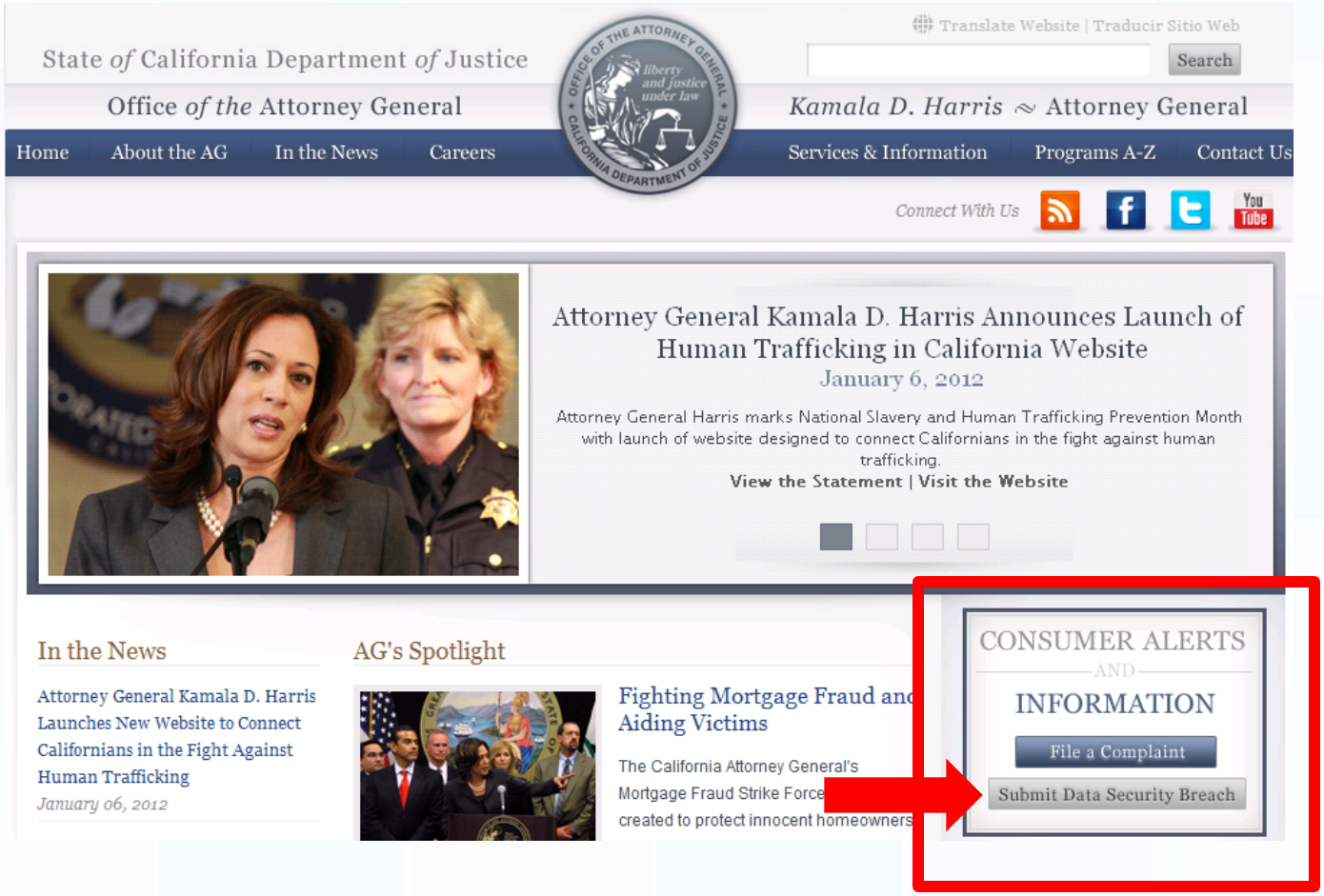
  www.leginfo.ca.gov

Legislative Update *(Continued)*

- SB 24 Actions
  - Continue to follow OIS SIMM 65D procedures, including use of existing templates and OIS notice review process
  - Review AG's New Procedures available on their website at: https://oag.ca.gov/ecrime/databreach/report-a-breach
  - Follow AG procedures when notice must be made to 500 or more individuals

Legislative Update *(Continued)*

- AG Procedures at http://oag.ca.gov/



Legislative Update *(Continued)*

- **AG Procedures**

Legislative Update *(Continued)*

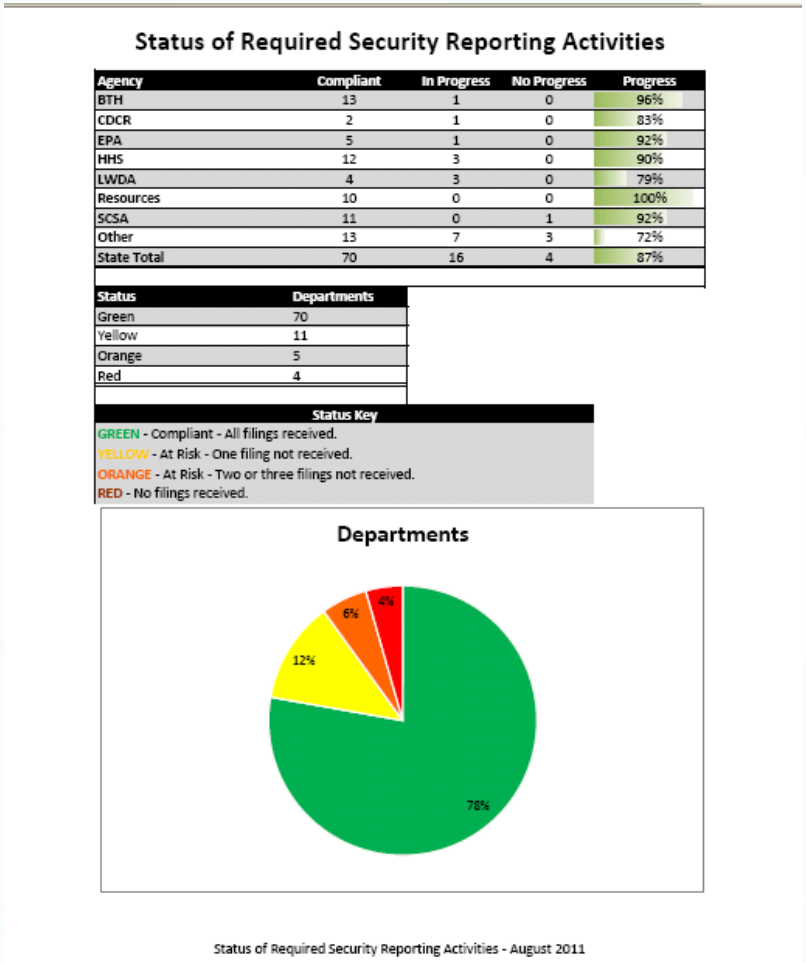
- AG Procedures
  - Required fields:
    - 2 - Org name and upload of breach notification
  - Optional fields (would like to have):
    - 19 – general breach data
    - 7 – law enforcement (not subject to FOIA/PRA)
- AG Process
  - eCrime Unit Staff look at submission
    - Pend publication, publish or do not publish
    - Validate uploaded documents (call & IP address)
    - Target turn-around is 48 hours

Policy Updates

- Tech Agency has established the Policy and Program Lifecycle Review Committee (PPLRC)
  - PPLRC is currently conducting a review of Tech Agency policies
- An IT Security Subcommittee is being established by the PPLRC
  - Subcommittee will review information security policy and program elements, and make recommendations

Status on Required Security Reporting Activities

- Annual Filings Due January 31
- Next publication February 2012
- Use January 2012 form version accessible at http://www.cio.ca.gov/OIS/Government/activities_schedule.asp



Status of Required Security Reporting Activities

Agency	Compliant	In Progress	No Progress	Progress
BTH	13	1	0	96%
CDCR	2	1	0	83%
EPA	5	1	0	92%
HHS	12	3	0	90%
LWDA	4	3	0	79%
Resources	10	0	0	100%
SCSA	11	0	1	92%
Other	13	7	3	72%
State Total	70	16	4	87%

Status	Departments
Green	70
Yellow	11
Orange	5
Red	4

Status Key

GREEN - Compliant - All filings received.
YELLOW - At Risk - One filing not received.
ORANGE - At Risk - Two or three filings not received.
RED - No filings received.

Departments

Status of Required Security Reporting Activities - August 2011

Required Annual Security Activities Reporting *(Continued)*

California Technology Agency
Office of Information Security

Annual Activity	Purpose	Value/Benefit to Agencies
Designation Letter	Ensure Agency has assigned personnel to fulfill key security and privacy roles and responsibilities. Also provides OIS ability to reach appropriate individuals for incident prevention, detection and response.	Receive notification of significant events affecting or potentially affecting them.
Risk Management and Privacy Program Compliance Certification	OIS mandate to track, monitor and report on state agency compliance with program requirements.	Statewide metrics and trends
Telework and Remote Access Security Compliance Certification	OIS mandate to track, monitor and report on state agency compliance with program requirements.	Statewide metrics and trends
Disaster Recovery Plan	Ensure Agency has a plan to recover critical/essential IT	Ability to minimize impact and recover within RTOs/MAOs

Training Resources

- 2012 ISO Basic Training Class Schedule
  - February 15
  - May 9
  - July 27
  - September 25
  - Register at OTech Events webpage: www.otech.ca.gov/calendar

Training Resources *(Continued)*

- **Free Online Training:**
  - **DHS/FEMA State Cyber Security Training**
    - Online, self–paced Cyber-Security training
    - Available at no charge to US citizens
    - http://www.teexwmdcampus.com/index.k2

IA General / Non-Technical:	IA Technical / IT Professional:	IA for Business Professionals:
➢ Information Security for Everyone ➢ Cyber Ethics ➢ Cyber Law and White Collar Crime	➢ Information Security Basics ➢ Secure Software ➢ Network Assurance Digital Basics	➢Business Information Continuity ➢Information Risk Management ➢Cyber Incident Analysis and Response

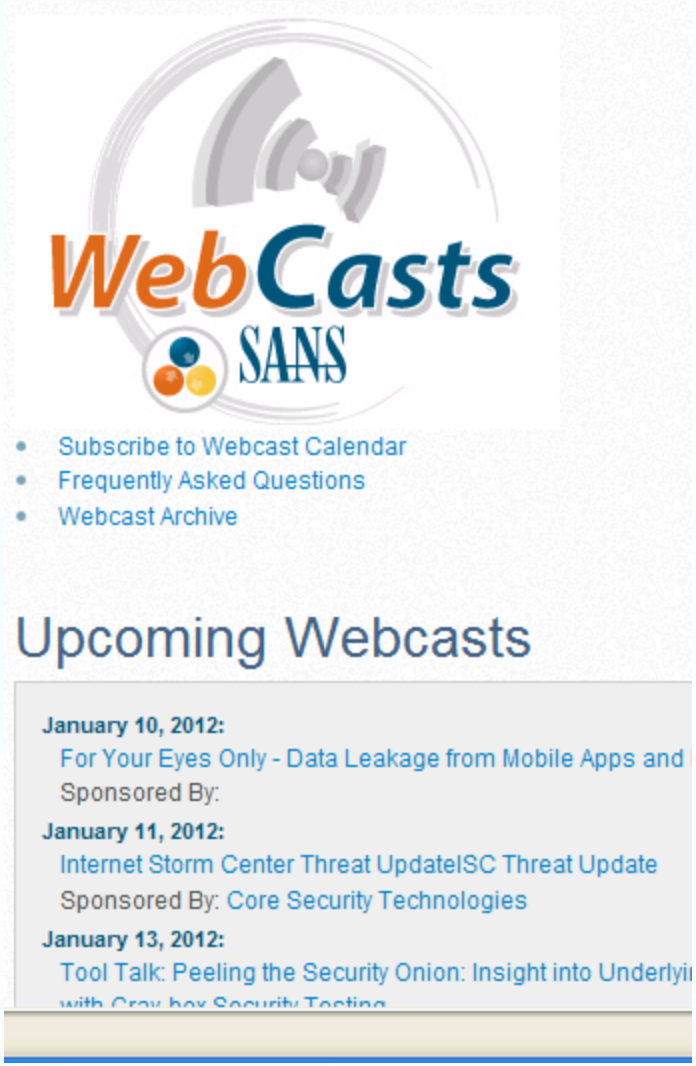
Training Resources *(Continued)*

- Free Online Training:
  - DoD Assurance Awareness Training
    - Online, self-paced or Order CD
    - http://iase.disa.mil/eta/online-catalog.html#iaatraining

General /Non-Technical:	Technical /IT Professional:	Business/Executives:
➢IA Awareness Training ➢Social Networking ➢Portable Electronic Devices /Removable Storage Media ➢Phishing ➢Personally Identifiable Information (PII)	➢IA Training for IA Professionals ➢IA Technical Training ➢Cyber Law Awareness ➢NetOps Training ➢FSO Tools Training ➢IA Simulations	➢IA Training for Senior Leaders ➢Information Assurance Awareness Shorts

Training Resources *(Continued)*

- Free Online Training:
  - SANS Institute Online Webcasts
  - http://www.sans.org/webcasts/
- MS-ISAC/SANS 2012 Aggregate Buy
  - http://msisac.cisecurity.org/resources/videos/sans-training.cfm



Training Resources *(Continued)*

- **Free Training for Law Enforcement:**
  - National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTOE)
    - Comprehensive digital evidence forensic examination training courses
    - NIJ Funded software tools
    - Online-interactive tools
  - http://www.ectcoe.net/

Training Resources *(Continued)*

- Government Mobility Forum:
  - February 8, 2012
  - Sacramento Convention Center
  - Free to government employees
  - Register at: www.governmentmobility.net

Free Awareness Resources

- DHS/MS-ISAC National Webcast Initiative
  - Next Webcast: Wednesday, February 22, 2011
  - Topic: Cyber Security Emerging Trends and Threats for 2012
  - All webcasts held from 2:00pm-3:00pm EST (11:00am-12 :00pm PST) http://msisac.cisecurity.org/webcast/
- Free Tools and Resources:
  - National Cyber Security Alliance http://staysafeonline.org/tools-resources

Future Meeting/Presentation Topics

- Proposed Topics:
  - Government Leaders:
    - DNS Security Project – OTech (March 2012)
    - eCrime Unit – AG (March 2012)
    - Enterprise GIS Project
  - Private Industry Partners:
    - Risk Assessment (February)
    - Security Metrics (March/April)

Statewide Program Updates

- Incident Management
  - Automation of Incident Reporting Process
    - Procurement Phase Completed!
    - Intent to Award Notice Made – No Protest
    - Project is moving to System Development Phase
  - Status of SIMM 65C Reviews
    - Delays in review and acknowledging receipt
    - Make sure they are complete
    - Many lack
      - Reference to OIS tracking number
      - Identification of root cause of incident
      - Corrective action that addresses root cause

Statewide Program Updates *(Continued)*

California Technology Agency Office of Information Security

- DR Management
  - DR Plan Reviews – Delays in review/feedback
  - Process Overview

All Submissions	Action Required Feedback on Last Full Submission	Feedback Pending on Last Full Submission
Email acknowledges receipt of plan submission.	If agency has received OIS feedback on its last full plan submission, and feedback indicated ACTION REQUIRED, then the agency needs to either submit another full plan, and/or remediation plan, that addresses the deficiencies that were identified by its next submission due date. The submission must be signed by the Director or designee.	If agency has not yet received OIS feedback on its last full plan submission (*before the next plan submission due date*) **and** there have been no changes to the environment that would warrant updates to the plan, then the agency may submit a "No-change Certification".

Statewide Program Updates *(Continued)*

California Technology Agency
Office of Information Security

- Risk Management
  - 99 SIMM 70C's received in 2011
    - 55% say they are fully compliant
    - 38% say they have a remediation plan to be fully compliant
  - Enterprise Risk Management Grant Project
    - NOT moving forward

National/Federal Initiatives

California Technology Agency
Office of Information Security

- **Federal Initiatives**
  - DHS Nationwide Cyber Security Review
    - Only one state did not respond
    - Aggregated results – Late Spring
  - DNS Policy Update
    - State CIO or Governor's designee will be POC
    - No change to advertising/political campaign ban
    - Required or strongly suggested for Federal entities: DNS Sec, IPV6, NSTIC, and MDM
    - Possibly required for States: DNS Sec
    - Nominal increase proposed .gov Domain
    - Advanced notice to be released in next 2 months

California Technology Agency
Office of Information Security

California Highway Patrol
Computer Crimes Investigations Unit

Sergeant Kelly Dixon

CCIU Discussion Topics

1. Hacktivism
2. Recent activity and attacks
   - Stratfor
   - CSLEA

California Technology Agency
Office of Information Security

Open Discussion

Friendly Reminders

FOUO Reminder:

- Follow FOUO Sensitive Information Handling Instructions
  - DON'T:
    - Post or make available on a public website
    - Provide to the media
  - DO:
    - Limit distribution and sharing to those that have a need to act on the information to protect information assets

Friendly Reminders *(Continued)*

ISO Meeting Changes Reminder:

- Registration is required so that we may:
  - More accurately account for the number of hand-outs /materials.
  - More easily track attendance/participation.
- A link will be sent to CIOs and ISO/ISO back-ups on designee list.
- **CIOs/ISOs may forward to others**

Friendly Reminders *(Continued)*

Feedback Survey Reminder:

- **The meeting survey will be emailed to you.**
- **Please complete.**
- **Your feedback is important to us!**

Closing

Thank you for joining us and all that you do!